

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
12835 (YO999-324)

Total Pages in this Submission

TO THE ASSISTANT COMMISSIONER FOR PATENTS

Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

METHOD AND APPARATUS FOR CONTROLLING E-MAIL ACCESS

and invented by:

Dimitri Kanevsky
Mariusz Sabath
Alexander Zlatsin

If a **CONTINUATION APPLICATION**, check appropriate box and supply the requisite information:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 37 pages and including the following:
 - a. ☒ Descriptive Title of the Invention
 - b. ☐ Cross References to Related Applications (if applicable)
 - c. ☐ Statement Regarding Federally-sponsored Research/Development (if applicable)
 - d. ☐ Reference to Microfiche Appendix (if applicable)
 - e. ☒ Background of the Invention
 - f. ☒ Brief Summary of the Invention
 - g. ☒ Brief Description of the Drawings (if drawings filed)
 - h. ☒ Detailed Description
 - i. ☒ Claim(s) as Classified Below
 - j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
12835 (YO999-324)

Total Pages in this Submission

Application Elements (Continued)

3. ☒ Drawing(s) (when necessary as prescribed by 35 USC 113)
- a. ☒ Formal Number of Sheets 4
- b. ☐ Informal Number of Sheets _____
4. ☒ Oath or Declaration
- a. ☒ Newly executed (original or copy) ☐ Unexecuted
- b. ☐ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional application only)
- c. ☒ With Power of Attorney ☐ Without Power of Attorney
- d. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application,
see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference (usable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied
under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby
incorporated by reference therein.
6. ☐ Computer Program in Microfiche (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all must be included)
- a. ☐ Paper Copy
- b. ☐ Computer Readable Copy (identical to computer copy)
- c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☒ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(B) Statement (when there is an assignee)
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Acknowledgment postcard
14. ☒ Certificate of Mailing
- ☐ First Class ☒ Express Mail (Specify Label No.): EM16995573US

**UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
12835 (YO999-324)

Total Pages in this Submission

Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)

16. ☒ Additional Enclosures (please identify below):

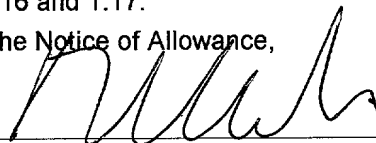
Associate Power of Attorney and Request for Change of Mailing Address

Fee Calculation and Transmittal

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	52	- 20 =	32	x \$18.00	\$576.00
Indep. Claims	3	- 3 =	0	x \$78.00	\$0.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
BASIC FEE					\$760.00
OTHER FEE (specify purpose) Assignment recordal fee					\$40.00
TOTAL FILING FEE					\$1,376.00

- ☐ A check in the amount of _____ to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. 50-0510/IBM as described below. A duplicate copy of this sheet is enclosed.
- ☒ Charge the amount of \$1,376.00 as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).


Signature

Richard L. Catania
Registration No. 32,608
SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza
Garden City, NY 11530
(516) 742-4343

Dated: October 21, 1999

CC:

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)Applicant(s): **Dimitri Kanevsky, et al.**

Docket No.

12835 (YO999-324)

Serial No.

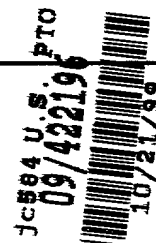
unassigned

Filing Date

herewith

Examiner

Group Art Unit

unassignedInvention: **METHOD AND APPARATUS FOR CONTROLLING E-MAIL ACCESS**I hereby certify that this **New Patent Application***(Identify type of correspondence)*

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under

37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231

on **October 21, 1999***(Date)***Janet Giordano***(Typed or Printed Name of Person Mailing Correspondence)**(Signature of Person Mailing Correspondence)***EM169955773US***("Express Mail" Mailing Label Number)***Note: Each paper must have its own certificate of mailing.**

METHOD AND APPARATUS FOR
CONTROLLING E-MAIL ACCESS

5 BACKGROUND OF THE INVENTION
 Field of the Invention

10 The present invention relates generally to e-mail messaging
 systems, and, particularly, to a system and methodology for
 controlling access to e-mail data content present in e-mail
 messages.

Discussion of the Prior Art

15 Senders of E-mail messages often want the message to be retrieved
 and accessed by the intended recipient and not made available to
 anybody else to access. For example, a sender of an e-mail
20 message including content of an intimate or personal nature would
 like to prevent a receiving user from showing his/her note to
 other people. Standard prevention methods that include encryption
 only helps to prevent unauthorized access to data while it is
 being communicated over the communication medium, e.g., phone
 lines. These security methods however, cannot prevent improper
25 use of messages at a receiving end after they are decrypted.

It would thus be highly desirable to provide a system and method that enables a sender to control access to e-mail data after sending the e-mail message to the intended recipient.

5 **Summary of the Invention**

It is an object of the present invention to provide a system and method for enabling a sender to control access to e-mail and electronic information content after sending the e-mail message to an intended recipient.

10 According to a preferred embodiment of the invention, there is
provided a system and method for controlling access to electronic
information packages including e-mail messages communicated from
a sending device to a device at one or more destination
15 locations. The system and method includes determining
fulfillment of one or more conditions at the destination
location; and, implementing controls in response to detection of
a fulfilled one or more conditions to enable access to content
provided in a communicated package. The access includes enabling
20 a user to perform certain operations (e.g., playing, displaying)
on the package content at the destination location, or,
preventing certain operations from being performed (e.g.,
copying, saving). A mechanism is included for enabling automatic

destruction of the e-mail messages immediately after being read
by an authorized recipient, or, after a predetermined time
interval from receipt of the message. A verification system is
additionally employed enabling a sender to verify and
5 authenticate users attempting to access the e-mail at the
destination location prior to authorizing use or playback of the
e-mail message.

Brief Description of the Drawings

10 Further features, aspects and advantages of the apparatus and
methods of the present invention will become better understood
with regard to the following description, appended claims, and
accompanying drawings where:

15 Fig. 1 is a general block diagram depicting the system for
controlling e-mail access by senders.

20 Fig. 2 is a diagram illustrating how a sender controls access to
his/her message at a receiving computer terminal.

Fig. 3 is an illustration depicting the window shell e-mail
message according to the invention.

Fig. 4 is an illustration depicting the electronic information package to be sent by the sender.

Fig. 5(a) is an illustration depicting the method implemented for remote authorization according to the invention.

Fig. 5(b) is an illustration depicting the method implemented for local authorization according to the invention.

Fig. 6 is an illustration depicting the general workflow process performed at the receiver terminal.

Detailed Description of the Preferred Embodiment

Figure 1 is a general block diagram depicting the system 10 for controlling e-mail access by senders. As shown in Figure 1, the system implements electronic devices for sending one or several electronic information packages 60 from one or several computer devices 12 at originating locations through communication channels 25a,b, such as telephone channels, wireless channels, radio links for delivery over a network, e.g., the Internet 19, to one or several computer devices 32 at destination locations. In the preferred embodiment, "electronic information packages" 60

include one or more of the following data types: e-mail messages, audio data, video data, animation data, textual data, pictorial data, which may include content of a confidential, personal, or intimate type. It is understood that an electronic information package may include any other types of data content, i.e., of a non-personal nature. According to the invention, the system enables access to these packages at the destination points and controls access to these packages at destination points by allowing or forbidding certain operations to be performed on these packages at these destination points in accordance with predetermined conditions. That is, only if certain predetermined conditions at these destination points are fulfilled, access to or destruction of these information packages is enabled.

It is understood that computer devices 12, 32 at originating and destination locations are devices that comprise CPU and memory storage devices (not shown) however, such devices 12, 32 may include: laptop/notebook computers, embedded devices, and consumer electronics (kitchen appliances, TV, electronic gadgets, palmtops, and telephones). Further, as shown in Figure 1, the sending terminal will include a memory or database storage device 14 comprising recipient verification/authentication data accessible by the sender as will be described herein.

As shown in Figure 1, the computer device 32 at the destination location includes a modified e-mail program or executor 47 for retrieving and notifying a recipient of a retrieved message. The recipient computer device 32 further includes a controller module 35 implementing software controls for preventing certain operations 37 from being performed on received electronic information packages in accordance with the invention as discussed herein. Such controls include the satisfaction and/or determination of one or more certain conditions, as will be described in greater detail herein. Particularly, the controller module 35 permits or prevents one or more of the following operations to be performed on the received electronic information packages: a saving operation for saving these packages in memory storage devices at destination points; a transfer operation such as copying, printing, storing or downloading of these packages and data to memory storage devices; a displaying operation for video data, text, picture and animation data on one or several display devices (not shown) at destination points; and, playing audio data on one or several audio playback/speaker devices 38 at destination points (as shown in Figure 1). It is understood that other operations such as the destruction of the received electronic package may be enabled or prevented by controller module 35. Alternately, the electronic information package

itself may be equipped with a program that is capable to control access to its content and destroy these packages when certain conditions are fulfilled. Thus, for instance, a sender system may be equipped with a program that is capable of controlling access to its content and destroy these packages when the certain conditions are fulfilled.

In a preferred embodiment, an electronic information package may be automatically destructed at the destination computer terminal 32 at a pre-determined time after it is received. Thus, as shown in Figure 1, a message destroyer process 46 which may be executing as part of the controller module, or separately therefrom, implements a timer mechanism 43 for determining time elapsed from receipt of the electronic information package at computer device 32. After one or more pre-determined time intervals has elapsed, the message destroyer mechanism 46 will automatically trigger a destruction operation in the computer terminal for deleting the electronic information package.

According to the invention, the number of intervals and length of a time interval may be set by the sender of the message, for instance, as a parameter to be entered as part of the e-mail message. As will be described in greater detail herein, this parameter information is received as part of or, in addition to the e-mail message, and implemented by the message destroyer 46

and timer mechanisms at the destination device 32. The actual destruction operation may be performed by the controller module 35 separately from or, in conjunction with a particular computer operating system.

5

It is understood that other conditions may be satisfied for triggering the destruction of a received electronic information package at the destination computer terminal. The other conditions include, but are not limited to the following: a) the detection of someone or something trying to perform a forbidden operation on the received electronic information package at the computer device 32; b) the direct command from the e-mail sender to instruct the control module to destroy a message at a later point in time; c) the detection of a modification or change in the CPU; a change in memory amount, or memory modification; a modification to or change of a peripheral device implemented at computer devices at destination points that are not related to the process of displaying or playing information packages at destination points; and d) the detection of when a playback and/or display of information package content is completed at the destination computer device 32.

Preferably, the condition a) of detecting attempted performance of a forbidden operation on the received electronic information package at the computer device 32 may be specified by the sender and entered as a parameter in the e-mail message, or, as a data attached to the message. As mentioned herein, types of forbidden operations include: a saving operation for saving these packages in memory storage devices at destination points; and, a transfer operation such as copying, printing, storing or downloading of these packages and data to memory storage devices. In operation, the control module 35 either separately from or, in conjunction with the computer device's operating system, will detect such a forbidden operation attempt, and trigger the destroyer process 46 to destruct the received electronic information package. Similarly, as for condition b) the sender may additionally send a direct command via e-mail at a later point in time as a parameter in the e-mail message, or, as data or a program attached to the message in order to trigger the destroyer process 46 to destruct the received electronic information package.

Preferably, the condition c) of detecting a modification or change in the CPU or a change/modification of memory or peripheral device may be specified by the sender of the package and performed by the control module 35. Once such a condition is

detected, the control module will trigger the destroyer process 46 to destruct the received electronic information package. Similarly, as for condition d) the control module 35 will trigger the destroyer process 46 to destruct the received electronic information package upon detection of a second or subsequent attempt to playback and/or display information package content at the computer device 32.

Still other conditions may be satisfied for triggering the destruction of a received electronic information package at the destination computer terminal. As shown in Figure 1, the other conditions include, but are not limited to the following: e) the detection of one or several processes running in CPU or memory devices at destination points 32 that are related to process of copying, downloading, printing, or saving information packages, or, f) the detection of pressing a certain key on a keyboard device 28, the pressing of a button, or the attempted use of other input devices (e.g., a speech recognition device, or a pen-table) at destination locations. As described above with respect to conditions c) and d), the detection of conditions e) and f) are performed by the control module 35 in conjunction with the computer's operating system, which cooperatively functions to

trigger the destroyer process 46 to destruct the received electronic information package at the receiver device 32.

In addition to specifying types of conditions for triggering the destruction of a received electronic information package at the destination computer terminal, the sender may specify one or more additional sets of conditions that must be satisfied for enabling the performance of certain operations on the received electronic information package at the destination location. As mentioned herein, types of permitted operations that may be performed include: but are not limited to, the following: a displaying operation for video data, text, picture and animation data on one or several display devices (not shown) at destination points; and, playing audio data on one or several audio playback/speaker devices 38 at destination points. The other conditions include, but are not limited to the following: g) a permission from the sender, e.g., entered as a parameter in the e-mail message, or, as a data or program attached to the message for use by the control module; and, h) the detection and identification of authorized user(s), for which access to these information packages is allowed; or, i) the detection or identification of other permissible electronic systems at destination locations

that are trying to perform operations on the received electronic package content.

As depicted in Figure 2, the condition h) of detecting and
5 identifying authorized user(s) to accomplish the detection of an
e-mail message, the computer device 32 at the destination
location and the sending device may include the monitoring of
user(s) via TV cameras or video camera devices 49 that are
installed at destination points. For example, video device
10 hardware/software devices, such as video camera 49, may be
implemented to enable a sender 12 to observe users that request
to read or play a content of information packages at destination
points.

15 In a preferred embodiment, an electronic information package
access operation may be enabled at the destination computer
terminal 32 by implementation of a identification/authentication
process 56 which executes locally as part of the controller
module 35, or remotely therefrom. The
20 identification/authorization process 56 that enables users or
systems to access information packages may be performed in
accordance with one or more of the following methods: the
presentation by a user of a "pid" (personal ID) and/or passwords;

and, the presentation and verification of that user's biometrics, fingerprints, and/or voice. That is, the identification/authorization process 56 implements well known techniques for verifying user's biometrics, fingerprints, and/or detected voice patterns at computer device 32. Such techniques for verifying, identifying may include techniques such as described in commonly-owned, co-pending U.S. Patent Application No. 09/079,754 (YO998-033 (728-103), entitled APPARATUS AND METHODS FOR USER RECOGNITION EMPLOYING BEHAVIORAL PASSWORDS, the whole contents and disclosure of which is incorporated by reference as if fully set forth herein.

The control module 35 additionally enables systems to access information packages and/or systems that request to access information packages such as: a) systems at communication subroutines/switches that support transferring data along other communication channels to new destination points; b) automated systems that are capable to understand content of information packages to perform necessary operations that are required by these sent packages; and, c) robotic devices. Thus, the identification/authorization process 56 further includes a detection mechanism for identifying if systems that are trying to perform operations on the received electronic package content at

destination points are permissible electronic systems. It is understood that the permissible electronic systems may be specified by a sender, e.g., entered as a parameter in the e-mail message, or, as a program attached to the message or information package.

According to the invention, access to electronic information packages is provided on displays 31, or, via speakers 38 or telephone sets 39, as shown in Figure 1. As shown in Figure 3, electronic information packages comprising visual, text, image, and/or pictorial data are displayed through window shells 59 according to known e-mail format or GUI representations, such as provided by Lotus Notes, Netscape, Microsoft Outlook, Eudora, and the like. However, it is understood that the window shell 59 will only display e-mail message content and prevent any further operations from being performed (no printing, copying, etc.). For instance, textual and pictorial data in window shells 59 may run from beginning of the data to the end (from one end of the window shell to another).

In accordance with the invention as illustrated in Figure 4, an electronic information package 60 may comprise one or more of the following fields: 1) a reading time field 62 having a data

structure which specifies the time in hours, minutes and seconds (HH:MM:SS) for when the message content is to be displayed or available for the recipient; 2) a Valid time interval field 64 (from <date:time> to <date:time>) which specifies the time range during which the message content may be read, i.e., if it is accessed before the specified time, the message will not be available, if expired, it will be automatically destroyed; 3) an authentication method field 66 which includes a description of the method implemented (either remotely or locally) for authenticating the recipient/user; 4) authentication data field 68 which includes data used for the verification method implemented, e.g., voice pattern, fingerprint and other biometric data; 5) the target recipient(s) field 70 which specifies one or more recipients allowed to access the message and their e-mail addresses; 6) a Sender field 72 which includes information about the person/system that sends the message; and 7) the actual body of the message 80, i.e., electronic information content.

The system for providing remote user authentication, according to the invention, is now described in view of Figure 5(a). As shown in Figure 5(a), at step 82, the message package is created on the sender system 12 and sent to the receiver terminal via communications channels 25. Preferably, the entire communication

between the sending and receiving end-points is encrypted. At
step 84, at the destination 32, the receiver device processes the
authentication method field 66 from the message package 60 and
determines the type of the authentication method and that the
5 authentication is to be performed remotely. After obtaining data
(e.g., by obtaining a user-entered userid or password, and/or a
camera image, voice-print, or a finger-print scan, etc.), the
collected information is communicated back to the sender device
at step 85 for processing there. Then, at step 86, a
10 verification of identity is be done by a query to the database 14
(Figure 1), visual inspection (by the active video camera system
(Figure 2), or by using apparatus for user recognition according
to techniques known in the prior art. When all the verification
conditions are fulfilled, at step 88, the sender will either
15 grant the access to the information by sending a message, or,
otherwise it may send a request to destroy the message. If
authentication is successful, the message package will be
available to the recipient for the period of time specified in
Reading Time field 62 (Figure 4), as indicated at step 89,
20 otherwise it will be destroyed, as indicated at step 90.

The system for providing local user authentication, according to
the invention, is now described in view of Figure 5(b). As shown

in Figure 5(b), at step 92, the message is created on the sender system 12. Further this step 92 requires determining a list of authorized recipient(s) and the authentication method, and the retrieval of authentication data from the database 14 (Figure 1) at the sender terminal. Once all this information is determined and all the data required for authentication is packaged with the message in the Authentication Data field 68, the message is then sent to the recipient terminal where it is received at step 94. At step 94, the authentication takes place and the results are compared with the data from the Authentication Data field 68. A decision is made at step 95 to determine if the authentication was successful. If the authentication was successful, the message becomes available to the recipient for the period of time specified in reading time field at step 96, otherwise it is destroyed at step 98.

It should be understood that, local authentication is much faster than remote authentication, because, after the message is sent, it executes independent of the sender.

Figure 6 is a workflow diagram illustrating the method executed at the receiver device for controlling e-mail access of the invention. As indicated at a first step 102, the message package

is received. Regardless of the type of the authentication specified in Authentication Method field 66, the receiver enables the authentication method at step 104 and compares the results with the data contained in Authentication Data field 68 of the received message, as indicated at step 106. If the authorization fails as indicated at 108, the destroy process is executed and the message content is destroyed. Likewise, if the validation fails as indicated at 110, the destroy process is executed. If the validation is accepted, the message content is available for display/playback. Once the message is displayed or played back, the reading time (HH:MM:SS) message field is checked and the timer mechanism invoked to enable display/playback of the message content for the specified time interval, as indicated at 118. If the reading message time has elapsed, as indicated at 115, the destroy process is executed and the message content destroyed. Likewise, the valid time interval is checked at 118 to determine if the recipient has accessed the message content within the valid time period indicated by the Valid time field 64 of the message. Once the valid time interval has elapsed as indicated at step 120, the message content is destroyed. Further, as shown in Figure 6, any illegal operation 121 causes the message to be destroyed and the sender to be optionally notified at step 123. Thus, a message is available to the recipient only when

successfully authenticated and only within the time period
specified in Reading Time field.

While the invention has been particularly shown and described
with respect to illustrative and preformed embodiments thereof,
it will be understood by those skilled in the art that the
foregoing and other changes in form and details may be made
therein without departing from the spirit and scope of the
invention which should be limited only by the scope of the
appended claims.

CLAIMS:

Having thus described our invention, what we claim as new, and desire to secure by Letters Patent is:

1 1. A system for controlling access to electronic information
2 packages communicated from a sending device to a device at one or
3 more destination locations, said system comprising:

4 means for determining fulfillment of one or more certain
5 conditions at said destination location; and,

6 control means responsive to detection of a fulfilled one or
7 more certain conditions for enabling access to content provided
8 in a communicated package, whereby said access includes enabling
9 a user to perform an operation on said package content at said
10 destination location.

11 2. The system as claimed in Claim 1, wherein said electronic
12 information packages include content comprising one or more of:
13 e-mail messages, audio data, video data, animation data, textual
14 data, and pictorial data.

1 3. The system as claimed in Claim 2, further including means
2 for automatically destroying a received electronic information

3 package in response to detection of a fulfilled one or more
4 certain conditions.

1 4. The system as claimed in Claim 3, wherein a fulfilled one or
2 more certain condition includes detection of one or more elapsed
3 time intervals, said system further comprising means for
4 determining elapsed time from receipt of an electronic
5 information package, said means generating a signal for
6 destroying the received electronic information package after a
7 time interval has elapsed.

8 5. The system as claimed in Claim 4, wherein said elapsed time
9 interval is specified by a sender at said sending device, said
10 electronic information package further comprising a specification
11 of one or more time-out intervals for use by said elapsed timing
12 means.

13 6. The system as claimed in Claim 5, wherein said operations
14 enabled to be performed on said package content at said
15 destination device include displaying one or more of video data,
16 text, picture and animation data via a display device at said
17 destination location.

1 7. The system as claimed in Claim 5, wherein said operations
2 enabled to be performed on said package content at said
3 destination device include playing audio data on one or several
4 speakers at said destination location.

1 8. The system as claimed in Claim 3, wherein said access includes
2 forbidding a user to perform an operation on said package content
3 at said destination device, said operations that are forbidden to
4 be performed on received information packages include one or more
5 of: saving, copying and downloading the received information
6 package content in a memory storage device and printing said
7 package content at said at a destination location.

1 9. The system as claimed in Claim 8, wherein said means for
2 determining fulfillment of one or more certain conditions at said
3 destination device further comprises means for detecting an
4 attempted performance of a forbidden operation at the destination
5 location, said destroying means automatically destroying a
6 received electronic information package in response to said
7 detection.

1 10. The system as claimed in Claim 8, wherein said means for
2 determining fulfillment of one or more certain conditions at said

3 destination device further includes means for receiving a direct
4 command signal from a sender at a sending device, said sender
5 command triggering destruction of said electronic information
6 package.

1 11. The system as claimed in Claim 8, wherein said means for
2 determining fulfillment of one or more certain conditions at said
3 destination device further comprises means for detecting changes
4 in physical hardware devices that are not related to the process
5 of displaying or playing information packages at destination
6 locations, said physical hardware devices including CPU, memory
7 or peripherals at said destination device, said destroying means
8 automatically destroying a received electronic information
9 package in response to said detection.

10 12. The system as claimed in Claim 8, wherein said means for
11 determining fulfillment of one or more certain conditions at said
12 destination device further comprises means for detecting a second
13 or repeated attempted to play or display information package
14 content, said destroying means automatically destroying a
15 received electronic information package in response to said
16 detection.

1 13. The system as claimed in Claim 9, wherein said means for
2 detecting an attempted performance of a forbidden operation at
3 the destination location, includes means operable in conjunction
4 with an operating system at said destination device, for
5 detecting invocation of one or several processes running in CPU
6 or memory at said destination location that are related to one or
7 more of: copying, downloading, printing, and saving, received
8 electronic information packages.

1 14. The system as claimed in Claim 9, wherein said means for
2 detecting an attempted performance of a forbidden operation at
3 the destination location, includes means operable in conjunction
4 with an operating system at said destination device, for
5 detecting a pressing of a key on a keyboard operable for said
6 destination device.

1 15. The system as claimed in Claim 1, wherein said means for
2 determining fulfillment of one or more certain conditions at said
3 destination location includes identification means for
4 identifying a user at said destination location for which access
5 to these information packages is allowed.

1 16. The system as claimed in Claim 15, wherein said
2 identification means includes video camera system for generating
3 video signals at said destination device and a display device for
4 receiving and displaying video signals at said sending device,
5 said video camera system enabling a sender at a sending device to
6 observe users attempting to read or play information package
7 content at a destination device.

1 17. The system as claimed in claim 15, wherein said
2 identification means for identifying a user at said destination
3 location comprises:

4 means for enabling users to present a password to said
5 system; and,

6 verification means for verifying a user's password prior to
7 enabling access to said information package.

1 18. The system as claimed in Claim 15, wherein said
2 identification means for identifying a user at said destination
3 location comprises means for enabling users to present a data for
4 authentication/verification that include one or more of the
5 following: biometrics, fingerprint, and voice data.

1 19. The system as claimed in Claim 1, wherein said means for
2 determining fulfillment of one or more certain conditions at said
3 destination location includes identification means for
4 identifying an electronic system at said destination location for
5 which access to these information packages is allowed.

1 20. The system as claimed in Claim 19, wherein said electronic
2 system trying to access information packages comprises a
3 communication process that supports transferring electronic
4 package content via a communication channel to new destination
5 locations.

1 21. The system as claimed in Claim 19, wherein said electronic
2 system trying to access information packages comprises an
3 automated process capable of understanding information package
4 content and performing necessary operations as required for
5 playing said content.

1 22. The system as claimed in Claim 19, wherein said electronic
2 system trying to access information packages comprises a robotic
3 device.

1 23. The system as claimed in Claim 1, wherein said electronic
2 information packages communicated from a sending device to a
3 device at one or more destination locations, is communicated over
4 a communications channel including one or more of: telephone
5 wires, wireless channels, radio links, network data connection.

1 24. A method for controlling access to electronic information
2 packages communicated from a sending device to a device at one or
3 more destination locations, said method comprising:

4 determining fulfillment of one or more conditions at said
5 destination location; and,

6 in response to determination of a fulfilled one or more
7 certain conditions, enabling access to content provided in a
8 communicated package.

9 25. The method as claimed in Claim 24, further including the
10 step of automatically destroying a received electronic
11 information package in response to detection of a fulfilled one
12 or more certain conditions.

1 26. The method as claimed in Claim 25, wherein a fulfilled one
2 or more certain condition includes detection of one or more

3 elapsed time intervals from receipt of an electronic package,
4 said method further comprising the steps of:
5 determining elapsed time from receipt of an electronic
6 information package; and,
7 generating a signal for initiating automatic destruction of
8 the received electronic information package after said elapsed
9 time interval.

1 27. The method as claimed in Claim 26, further including the step
2 of enabling a sender to specify said time interval.

3 28. The method as claimed in Claim 24, wherein said step of
4 enabling access to said content of said communicated package
5 includes enabling a user to display one or more of video data,
6 text, picture and animation data via a display device at said
7 destination location, and play audio data on one or several
8 speakers at said destination location.

1 29. The method as claimed in Claim 28, wherein said step of
2 enabling access to said content of said communicated package
3 includes forbidding a user to perform an operation on said
4 package content at said destination device, said operations
5 forbidden to be performed on received information packages

6 including one or more of: saving, copying and downloading the
7 received information package content in a memory storage device
8 and printing said package content at said at a destination
9 location.

1 30. The method as claimed in Claim 28, wherein said step of
2 determining fulfillment of one or more conditions at said
3 destination device further comprises detecting an attempted
4 performance of a forbidden operation at the destination location;
5 and, in response to said detecting, automatically destroying a
6 received electronic information package.

7 31. The method as claimed in Claim 28, wherein said step of
8 determining fulfillment of one or more conditions at said
9 destination device further includes: receiving a direct command
10 signal from a sender at a sending device for initiating
11 destruction of said electronic information package.

1 32. The method as claimed in Claim 28, wherein said step of
2 determining fulfillment of one or more conditions at said
3 destination device further includes: detecting changes in
4 physical hardware devices that are not related to the process of
5 displaying or playing information packages at destination

6 locations, said physical hardware devices including CPU, memory
7 or peripherals at said destination device, and in response to
8 said detecting, automatically destroying a received electronic
9 information package.

1 33. The method as claimed in Claim 28, wherein said step of
2 determining fulfillment of one or more conditions at said
3 destination device further includes: detecting a second or
4 repeated attempted to play or display information package
5 content, and in response to said detecting, automatically
6 destroying a received electronic information package.

1 34. The method as claimed in Claim 30, wherein said step of
2 detecting an attempted performance of a forbidden operation at
3 the destination location includes: detecting invocation of one or
4 several processes running in CPU or memory at said destination
5 location that are related to one or more of: copying,
6 downloading, printing, and saving, received electronic
7 information packages.

1 35. The method as claimed in Claim 30, wherein said step of
2 detecting an attempted performance of a forbidden operation at

3 the destination location includes: detecting a pressing of a key
4 on a keyboard operable for said destination device.

1 36. The method as claimed in Claim 24, wherein said step of
2 determining fulfillment of one or more certain conditions at said
3 destination location includes the step of: identifying a user at
4 said destination location for which access to these information
5 packages is allowed.

1 37. The method as claimed in Claim 36, wherein said identifying
2 step includes implementing video camera device for generating
3 video signals at said destination device for receipt by said
4 sender, said sender receiving and displaying video signals at
5 said sending device for identifying users attempting to read or
6 play information package content at a destination device.

1 38. The method as claimed in Claim 37, wherein said identifying
2 step further includes:

3 enabling users to present a password to said method; and,
4 verifying a user's password prior to enabling access to said
5 information package.

1 39. The method as claimed in Claim 37, wherein said identifying
2 step further includes authenticating said user by enabling
3 users to present biometric data on/verification that include one
4 or more of the following: biometrics, fingerprint, and voice
5 data, said method including comparing input biometric data with
6 predetermined biometric data corresponding to the intended
7 recipient.

1 40. The method as claimed in Claim 24, wherein said step of
2 determining fulfillment of one or more conditions at said
3 destination location includes identifying an electronic system at
4 said destination location for which access to these information
5 packages is allowed.

1 41. A program storage device readable by a machine, tangibly
2 embodying a program of instructions executable by the machine to
3 perform method steps for controlling access to electronic
4 information packages communicated from a sending device to a
5 device at one or more destination locations, said method steps
6 comprising:

7 determining fulfillment of one or more conditions at said
8 destination location; and,

9 in response to determination of a fulfilled one or more
10 certain conditions, enabling access to content provided in a
11 communicated package.

1 42. The program storage device as claimed in Claim 41, further
2 including the step of automatically destroying a received
3 electronic information package in response to detection of a
4 fulfilled one or more certain conditions.

1 43. The program storage device as claimed in Claim 42, wherein a
2 fulfilled one or more certain condition includes detection of one
3 or more elapsed time intervals from receipt of an electronic
4 package, said method further comprising the steps of:

5 determining elapsed time from receipt of an electronic
6 information package; and,

7 generating a signal for initiating automatic destruction of
8 the received electronic information package after said elapsed
9 time interval.

1 44. The program storage device as claimed in Claim 43, wherein
2 said step of determining fulfillment of one or more conditions at
3 said destination device further comprises detecting an attempted
4 performance of a forbidden operation at the destination location;

5 and, in response to said detecting, automatically destroying a
6 received electronic information package.

1 45. The program storage device as claimed in Claim 43, wherein
2 said step of determining fulfillment of one or more conditions at
3 said destination device further includes: receiving a direct
4 command signal from a sender at a sending device for initiating
5 destruction of said electronic information package.

1 46. The program storage device as claimed in Claim 43, wherein
2 said step of determining fulfillment of one or more conditions at
3 said destination device further includes: detecting changes in
4 physical hardware devices that are not related to the process of
5 displaying or playing information packages at destination
6 locations, and in response to said detecting, automatically
destroying a received electronic information package.

1 47. The program storage device as claimed in Claim 43, wherein
2 said step of determining fulfillment of one or more conditions at
3 said destination device further includes: detecting a second or
4 repeated attempted to play or display information package
5 content, and in response to said detecting, automatically
6 destroying a received electronic information package.

1 48. The program storage device as claimed in Claim 43, wherein
2 said step of detecting an attempted performance of a forbidden
3 operation at the destination location includes: detecting
4 invocation of one or several processes running in CPU or memory
5 at said destination location that are related to one or more of:
6 copying, downloading, printing, and saving, received electronic
7 information packages.

1 49. The program storage device as claimed in Claim 43, wherein
2 said step of detecting an attempted performance of a forbidden
3 operation at the destination location includes: detecting a
4 pressing of a key on a keyboard operable for said destination
5 device.

1 50. The program storage device as claimed in Claim 43, wherein
2 said step of determining fulfillment of one or more certain
3 conditions at said destination location includes the step of:
4 identifying a user at said destination location for which access
5 to these information packages is allowed.

1 51. The program storage device as claimed in Claim 50, wherein
2 said identifying step includes:
3 enabling users to present a password to said method; and,

4 verifying a user's password prior to enabling access to said
5 information package.

1 52. The program storage device as claimed in Claim 50, wherein
2 said identifying step includes authenticating said user by
3 enabling users to present biometric data on/verification that
4 include one or more of the following: biometrics, fingerprint,
5 and voice data, said method including comparing input biometric
6 data with predetermined biometric data corresponding to the
7 intended recipient.

METHOD AND APPARATUS FOR CONTROLLING E-MAIL ACCESS

ABSTRACT OF THE DISCLOSURE

5 A system for controlling access to electronic information
packages including e-mail messages communicated from a sending
device to a receiving device at one or more destination
locations. The system and method includes determining
fulfillment of one or more certain conditions at the destination
10 location; and, implementing control in response to detection of a
fulfilled one or more certain conditions to enable access to
content provided in a communicated package. The access includes
enabling a user to perform certain operations on the package
content at the destination location, or, preventing certain
15 operations from being performed. A mechanism is included for
enabling automatic destruction of the e-mail messages immediately
after being read by an authorized recipient, or, after a
predetermined time interval from receipt of the message. A
verification system is employed enabling a sender to verify users
20 attempting to access the e-mail.

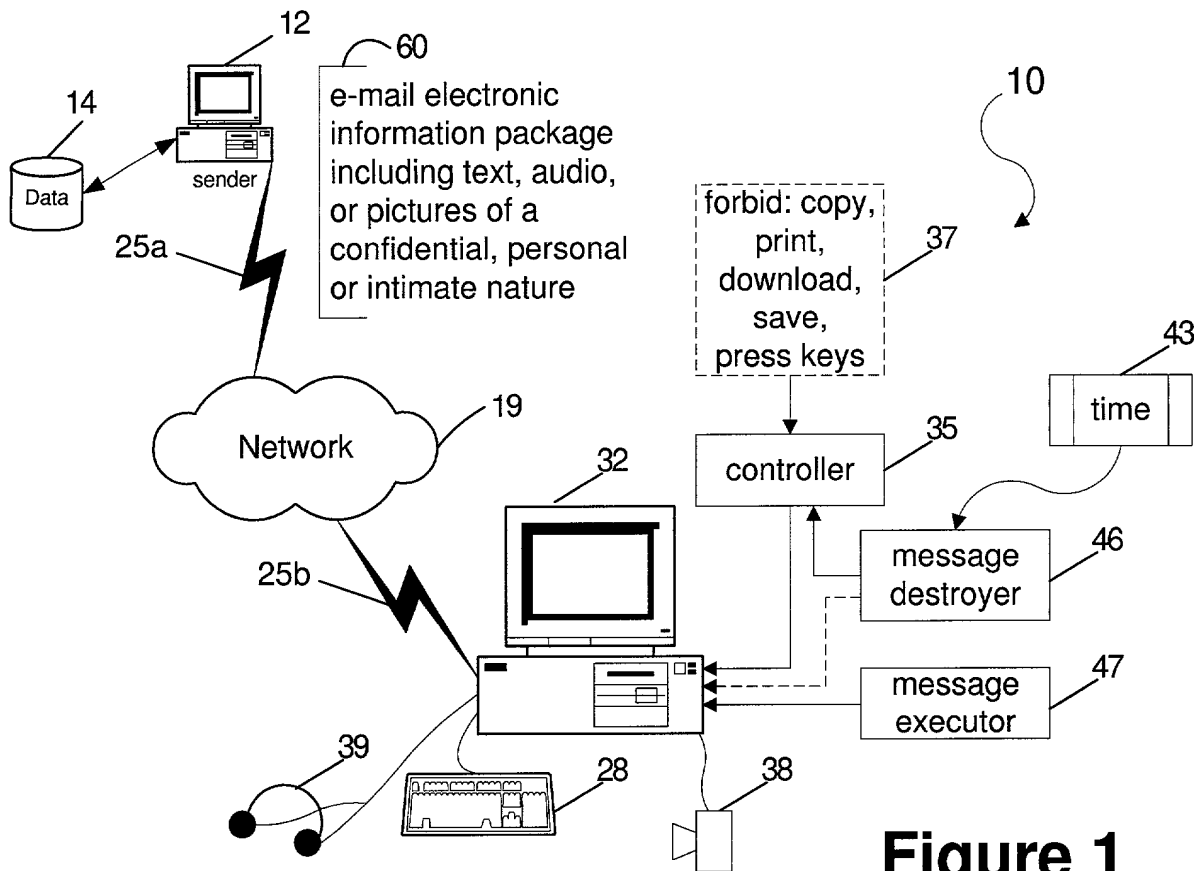


Figure 1

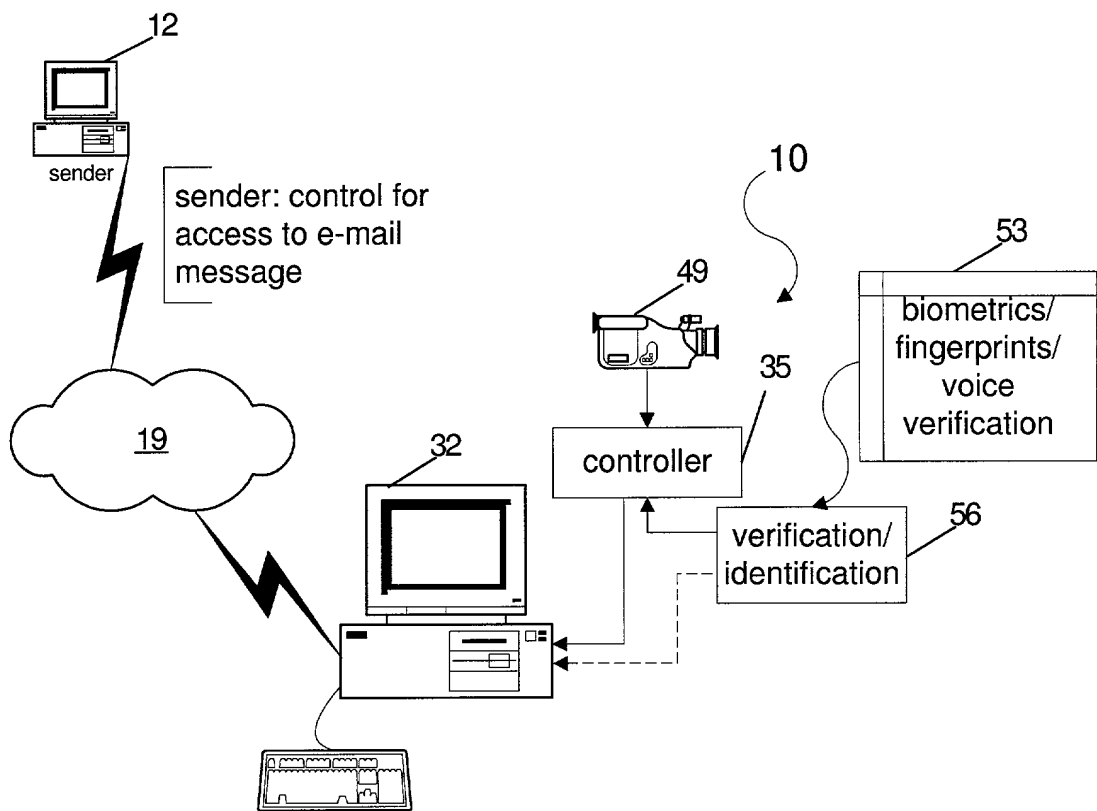


Figure 2

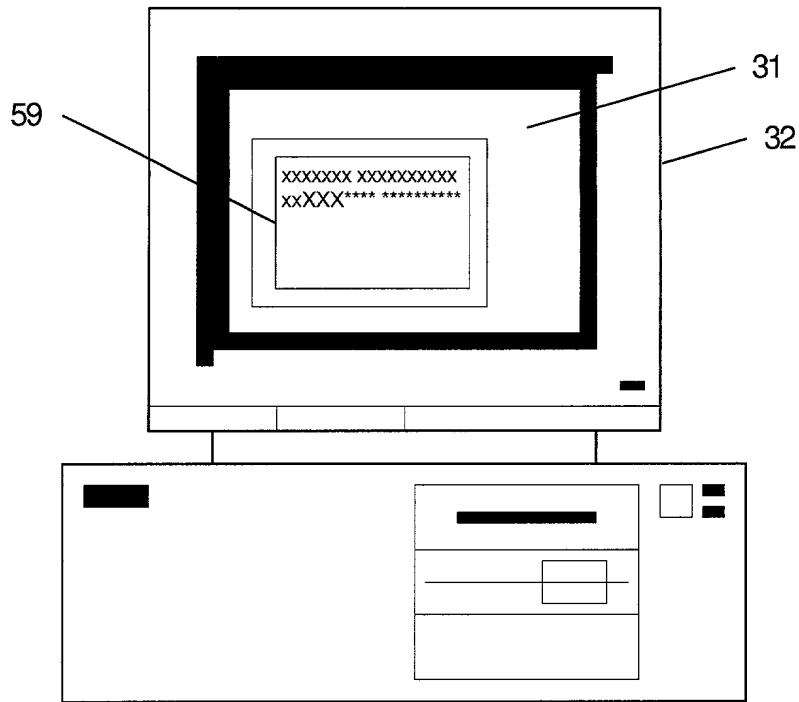


Figure 3

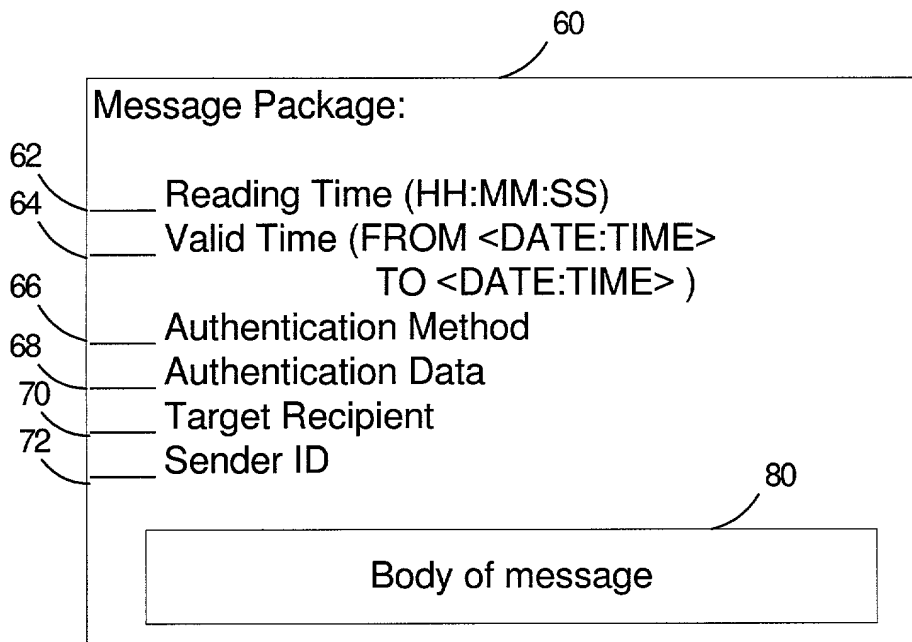


Figure 4

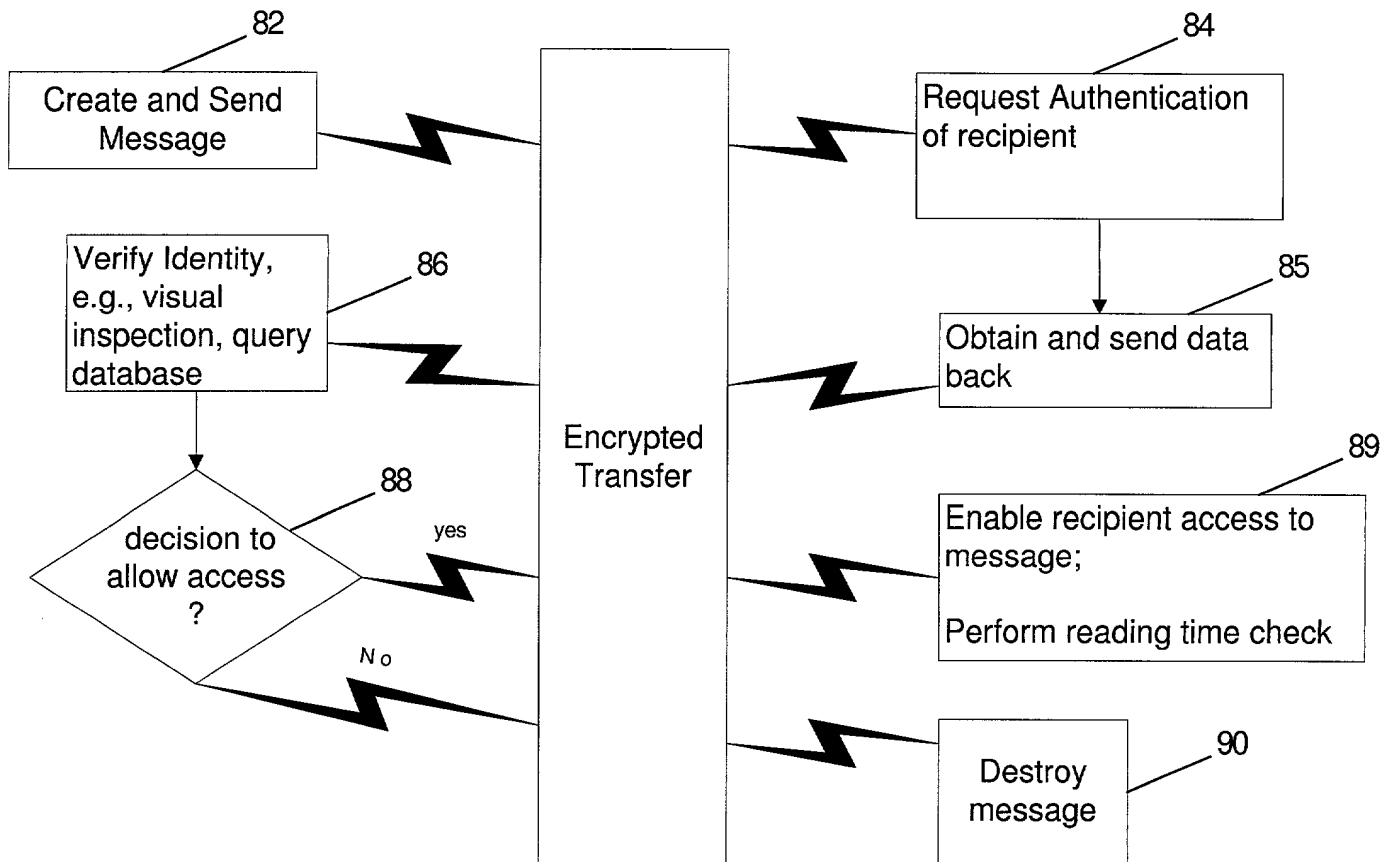


Figure 5(a)

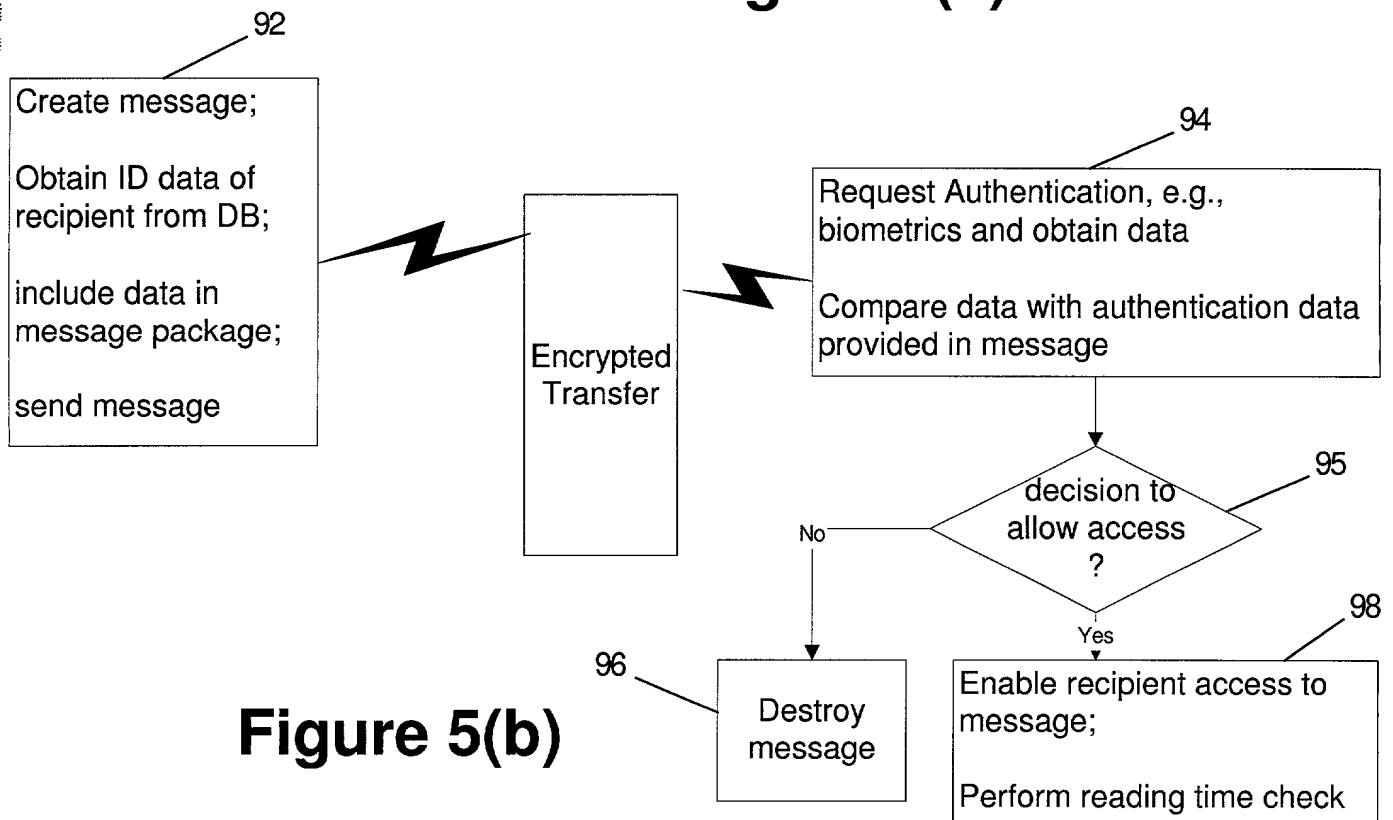


Figure 5(b)

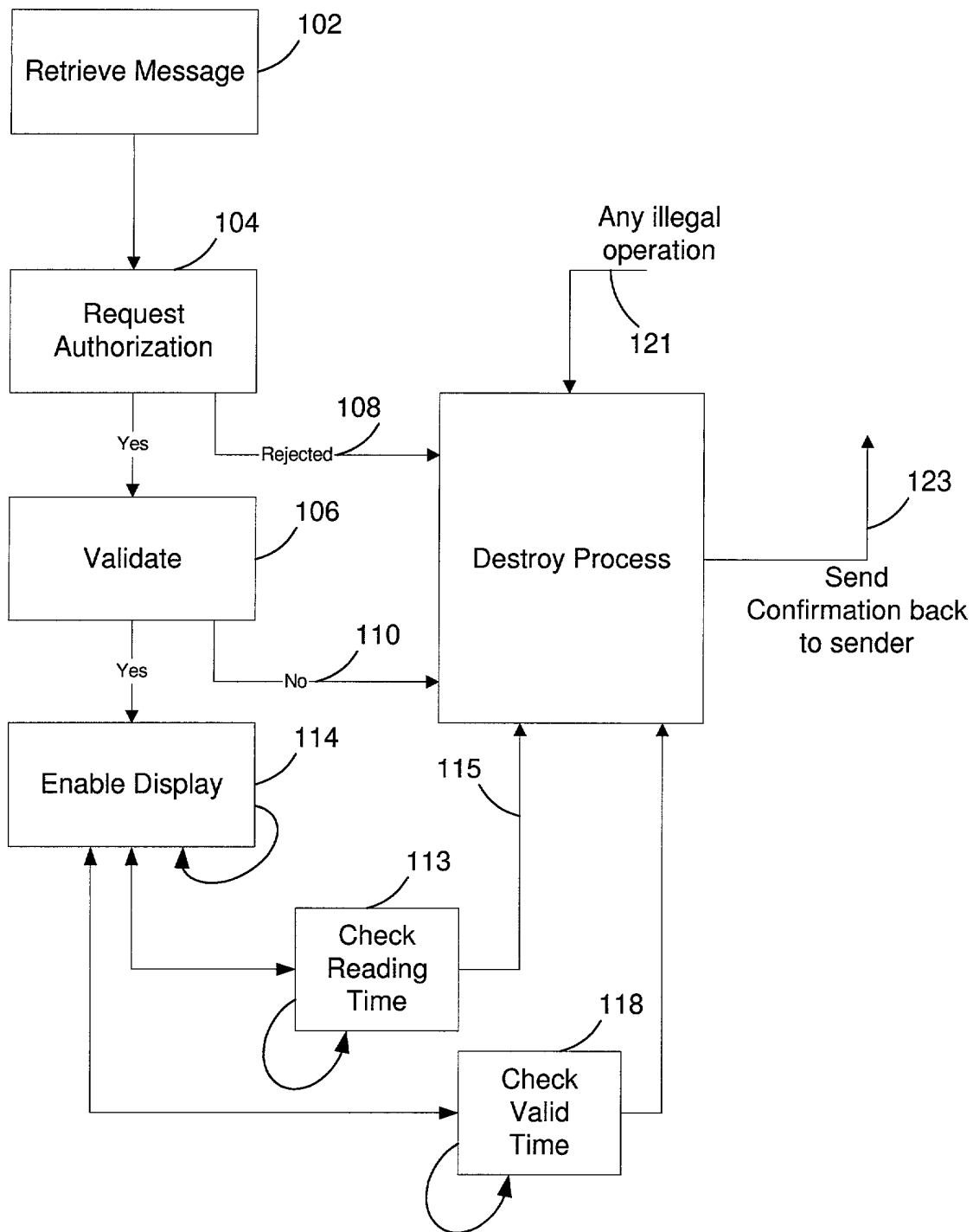


Figure 6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Dimitri Kanevsky et al. **Docket:** 12837 (YO999-324)

Serial No.: Unassigned

Dated: October 4, 1999

Filed: Herewith

For: METHOD AND APPARATUS FOR CONTROLLING
E-MAIL ACCESS

Assistant Commissioner for Patents
Washington, DC 20231

**ASSOCIATE POWER OF ATTORNEY AND
REQUEST FOR CHANGE OF MAILING ADDRESS**

Sir:

Applicants, by their attorneys of record, hereby
grant an Associate Power of Attorney to:

RICHARD L. CATANIA, Reg. No. 32,608; FRANK S. DIGIGLIO, Reg.
31,346; KENNETH L. KING, Reg. No. 24,223; STEPHEN D. MURPHY,
Reg. No. 22,002; LEOPOLD PRESSER, Reg. No. 19,827; and JOHN S.
SENSNY, Reg. No. 28,757

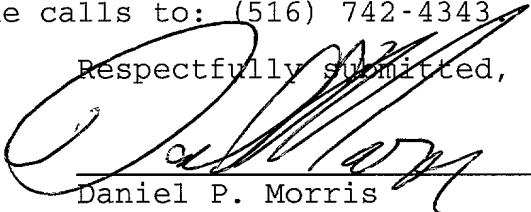
with full power of substitution to prosecute this application
and transact all business in the United States Patent and
Trademark Office in connection therewith.

Applicants further request that all future
correspondence in connection with this application be directed
and addressed to:

RICHARD L. CATANIA, ESQ.
SCULLY, SCOTT, MURPHY AND PRESSER
400 Garden City Plaza
Garden City, New York 11530

Direct all telephone calls to: (516) 742-4343

Respectfully submitted,


Daniel P. Morris
Registration No.: 32,053
Telephone No.: (914) 945-3217

IBM Corporation
T.J. Watson Research Center
Route 134/Kitchawan Road
P.O. Box 218
Yorktown Heights, New York 10598
SF/vjs

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND APPARATUS FOR CONTROLLING E-MAIL ACCESS

the specification of which (check one)

X is attached hereto.

_____ was filed on _____ as United States Application Number _____

or PCT International Application Number _____

and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

_____ (Application Number)	_____ (Filing Date)
_____ (Application Number)	_____ (Filing Date)

I hereby claim the benefit under 35 U.S.C. §120 of any United States Application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States, or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 CFR §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status) (patented, pending, abandoned)
_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (list name and registration number).

Manny W. Schecter (Reg. 31,722), Terry J. Ilardi (Reg. 29,936), Christopher A. Hughes (Reg. 26,914), Edward A. Pennington (Reg. 32,588), John E. Hoel (Reg. 26,279), Joseph C. Redmond, Jr. (Reg. 18,753), Douglas W. Cameron (Reg. No. 31,596), Wayne L. Ellenbogen (Reg. No. 43,602), Stephen C. Kaufman (Reg. No. 29,551), Daniel P. Morris (Reg. No. 32,053), Louis J. Percello (Reg. No. 33,206), Jay P. Sbrollini (Reg. No. 36,266), David M. Shofi (Reg. No. 39,835), Robert M. Trepp (Reg. No. 25,933) and Louis P. Herzberg (Reg. No. 41,500).

Send Correspondence to: Richard L. Catania, Scully, Scott, Murphy & Presser

400 Garden City Plaza, Garden City, New York 11530

Direct Telephone Calls to: (name and telephone number) Richard L. Catania, (516) 742-4343

Dimitri Kanevsky

Full name of sole or first inventor

D Kanevsky

Inventor's Signature

10/18/99

Date

1358 Spring Valley Road, Ossining, NY 10563

Residence

USA

Citizenship

Same as above

Post Office Address

Mariusz Sabath

Full name of second joint inventor, if any

Mariusz Sabath

Inventor's signature

10/18/99

Date

60 Morrow Avenue, Apt., 4LS, Scarsdale, NY 10583

Residence

Polish

Citizenship

Same as above

Post Office Address

Alexander Zlatsin

Full name of third joint inventor, if any

Alexander Zlatsin

Inventor's Signature

10/18/99

Date

648 Kessler Place, Yorktown Heights, NY 10598

Residence

USA

Citizenship

Same as above

Post Office Address